A study of Different Attacks on Localization in WSN

Yogendra N. Suralkar
Research Scholar, IT Department
SCOE, Vadgaon(Bk)
Pune, Maharashtra, India
yogenns@gmail.com

Ganesh R. Pathak
Associate Professor, IT Department
SCOE, Vadgaon(Bk)
Pune, Maharashtra, India
pathak.gr@gmail.com

***Abstract* - Over the last decade Wireless Sensor Networks (WSNs) have gained a lot of attention. WSN is a network of distributed mobile nodes used to monitor physical conditions. They are easy to deploy in hard terrain and require no centralized infrastructure. Determining the actual location of the sensor node is important task along with verifying the location. Localization needs to be secured from numerous threats.**

In this paper we will discuss different types of attacks on Localization in WSN. We will list out the work done in thwarting these attacks. We will also discuss some secure localization algorithms.

Keywords- WSN, Localization, Attacks,

I. INTRODUCTION

Wireless Sensor Network is a heterogeneous network composed of a large number of small, low-cost, battery constrained devices called sensor nodes and few general purpose computing devices referred to as base stations. A sensor node is able to observe condition values of a certain area like temperature, sound, vibration, pressure, motion or pollutants. These sensor nodes are deployed in harsh terrain called sensor field with no central infrastructure.

Determining the position of these sensor nodes is very essential for applications like surveillance networks. We could use GPS to track all these sensor nodes that will mean installing GPS on thousands of sensor nodes. Also, these nodes have little battery which will be drained by the GPS module.

For these we use localization schemes to determine the physical location of the sensor node if no special tracking hardware is available. Many localization scheme use anchor based approach where they assume that a certain number of sensor nodes called anchors know their actual physical location. These algorithms then calculate the location of other sensor nodes relative to these anchors. Some other schemes do not use anchors. Instead, they calculate the position of the sensor nodes based on virtual coordinates.

Now, these WSNs are not secure and can be attacked by adversaries. An attack on WSN can affect the localization and will result in getting wrong position of a sensor node. Attacks like Black hole, worm hole, grey hole sink hole will increase loss of packets which will make location determining very difficult [1][2]. The distance fraud and terrorist fraud attack will result in wrong measurements of a given sensor node in the sensor field [3].

In order to detect and prevent threats to security we need to understand all these attacks and act accordingly. Many researchers have proposed ways to deal with these attacks. We will discuss these attacks and defenses in this paper. Section II will discuss the security goals in WSN along with security related issues. In Section III we will list out different attacks in WSN. Section IV will give the secure localization schemes available followed by the Conclusions sections.

II. SECURITY IN WSN: GOALS AND ISSUES

To ensure security of any network some rules need to be followed. These rules are the primary goals and security can only be assured if all these goals meet. These goals are Confidentiality, Integrity, Availability and Authenticity [4]. Besides, these there are secondary goals which are Data Freshness, Self-Organization, and Time Synchronization. Secure Localization. We will see these goals in detail.

A. Confidentiality

Confidentiality is the ability to provide access of information to only the authorized users. If the information gets in the hand of unauthorized user or attacked, it can be used against the network. In case of localization if the node's position gets revealed to the attacker can locate the sensor node and may harm it. Confidentiality is achieved by encrypting the information which can only be decrypted by authorized users only.

B. Integrity

Integrity means data send is received with any modifications. Loss of integrity means data has been changed by an attacker and if the change is not detected it could pose a serious threat to network. In case of spoofing attack, Manipulation attack [3] modifies the data in order to attack the network.

C. Availability

Availability ensures that information is accessible by legitimate user at any given time. Black hole and Worm hole attack which cause packet loss threatens this goal as receiver does not receive the data.

D. Authenticity

It verifies if the said user is who he claims to be. Sometimes attacker tries to mix up with the network by posing as another user it is called Sybil attack. Mafia fraud attack which is a man-in-the-middle attack threatens the authenticity as it poses as legitimate entity can causes wrong measurement of sensor node's position.

The secondary goals are as listed below.

E. Data Freshness

It suggests that data is fresh and it not expired or replayed. Some attacks like Reply attack use the data from communication between some other nodes and use it fake their identity. These old messages are sent over and over again which can be overcome by using time stamps or sequence numbers.

F. Self-Organization

A these wireless sensor networks have no centralized system, managing them should be done by node itself. This is called as Self-organizing or Self-healing.

G. Time Synchronization

Any two sensor nodes should be time synchronized as they will be computing the end-to-end delay or data freshness based on time stamps. These results will get wrong if the two nodes have different time.

H. Secure Localization

We will be focusing on securing the localization process i.e. determining the actual physical positions of the sensor node. It is important to get right location as it will directly lead us to the sensor node which has found the fault.

III. ATTACKS ON WIRELESS SENSOR NETWORKS

Wireless Sensor Network is prone to different attacks. These attacks can occur at any layer of network. In this section we will list out different attacks which can harm the localization process.

A. Distance Fraud Attack

A distance fraud attack is based on hacking the method of determining the actual physical position. In this attack the malicious node tries to appear closer or further in order change its actual position. This attack is conducted by manipulation the signal strength of the malicious node. If the signal strength is high, the malicious node appears closer and if the strength is low, the malicious node appears further.

The distance fraud harms the localization process as the nodes whose position is calculated by referencing malicious node actually have different position.

B. Mafia Fraud Attack

It is a man-in-the-middle attack where a malicious node inserts itself in a location verification process. As shown in figure 1 the intruder poses as a verifier to the node whose identity is to be checked and prover to the node who is verifying the identity. It takes the location packet from verifier pretending to be prover and forwards it to real prover by pretending to be verifier. The prover acknowledges the packet and sends ACK packet through the intruder to the verifier which causes the verifier to compute the location incorrectly.

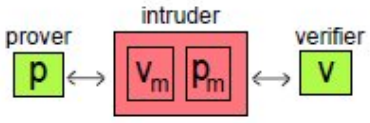

Figure 1 Mafia Fraud Attack

C. Terrorist Fraud Attack

A terrorist fraud attack is similar to the mafia fraud attack except that here the prover is cooperating with intruder to make it look closer. The packets addressed to the prover which go through intruder which will acknowledge it instantly making the prover appear closer.

D. Wormhole Attack

A wormhole is a low-latency junction between two sections of a network. The malicious node receives packets in one section of the network and sends them to another section of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location.

E. Black hole Attack

Black hole is a malicious node which advertises to its neighboring nodes that it has the shortest path to the destination. Once a neighbor starts sending data packets through that path, black hole drops all the packets it receives as shown in figure 2. This creates a serious issue of Denial of Service as the sender will claim the packet is sent but receiver will never get that packet.

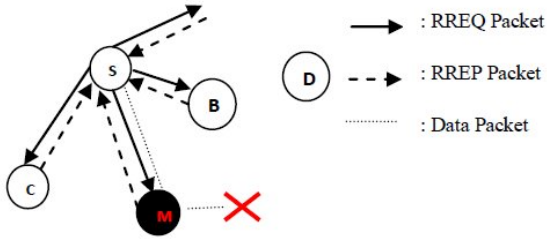

Figure 2 Black hole Attack

This attack prevents the verifier node from getting the location of the sensor nodes.

F. Sybil Attack

In Sybil attack the malicious node presumes multiple identities to confuse the network and to make the network unstable. If the attacker defects the anchor node (a node which knows its actual position and is used for reference to measure other node's position) then localization scheme will result in wrong measurements.

G. Jamming

Jamming is a physical layer attack where communication is interrupted by blocking the signal. Jamming can be of two types – constant jamming where complete network is down and intermittent jamming where nodes are able to communicate periodically not continuously.

H. Overshadowing

In this attack the adversary has far more signal strength than that of the sensor node. When sensor node sends its message the signal looks like noise in the presence of much stronger signal of the adversary. The receiver discards the original message thinking it is just noise which creates denial of service.

I. Manipulation

Manipulation breaks the integrity of the network by modifying the messages sent between sensor nodes. The malicious node intercepts the message being passed between two sensor nodes and modifies it. This makes the message lose its integrity. This is very harmful as the malicious node can change the location information. This can be prevented by adding parity bits for detection of modification

J. Replay

In this attack the malicious node sends the previous messages for new communication. It harms the data freshness of the network. The replayed message could be intercepted by any legitimate communication

K. Homing

In homing, attacker gets the physical location of the sensor nodes or cluster heads by intercepting location messages or analyzing the traffic and signal strength. After getting the physical location, attacker destroys the nodes physically and cause further network destruction.

L. Spoofing

This attack create false path by analyzing the routing information and then modifying it. The newly created path lengthens or shortens the source routes, generates false message which could lead to wrong location measurements.

M. Hello Flood Attacks

It uses HELLO message to advertise itself to the adjoining nodes. The malicious node uses high transmission range to send HELLO packets which cause the sensor node to think of malicious nodes as their neighbor. The nodes send packets through the malicious node but instead the packets get lost as the malicious node is outside of their range. When the nodes do not get acknowledge they resend the packet which creates a flood of HELLO packets in the network. This problem leads to network congestion. When such congestion occur the verifier gets the packets later than expected which results in wrong location computation.

IV. SECURE LOCALIZATION SCHEMES

With different attacks threatening the security of the wireless sensor network we need some secure methods to measure the physical position of the nodes. Despite the attack the network should be able to get proper location. In this section we will discuss different methods that will ensure robust location estimation.

A. SeRLoc

In paper [5], the authors Lazos and Poovendran propose a method called Secure Range Independent Localization Scheme (SeRLoc). It is an anchor based scheme where the network consists of two types of nodes-sensors which are unknown of their positions and locators which are aware of their location. SeRLoc is very simple where sensor nodes communicate with nearby locators to get an intersection point. The centroid of this intersection is estimated to be the location of the given sensor. To ensure the safety of this algorithm authors have discussed security measures for 3 basic attacks viz. wormhole, Sybil and compromised entities.

1) Wormhole attack

Here, the beacons sent from locator are sent to far sensor. The wormhole attack is first detected by using one of the two methods

Single message per locator/sector property- which means if the sensor is in the range of locator it will receive two message one from locator and one from wormhole tunnel. So wormhole is detected.

Communication range constraints property where the distance from sensor to locator is constrained to a specific distance, say R. if a sensor two messages from a locator more than 2R apart i.e. if the time between two message takes more time than 2R it detects the wormhole.

Once the wormhole is detected it uses ACLA (Attach to Closer Locator Algorithm) to recover. In ACLA the sensor node assumes the locator which replies first is closest and which locator does not intersect with it is the wormhole and hence discarded.

2) Sybil Attack

In Sybil attack multiple identities of locators are created which exceeds the locator density value initially stored in sensor nodes. Once the Sybil attack is detected ACLA is used to recover from it.

3) Compromised network Entities

In this attack locator is compromised and ACLA will not work. Instead ELRA (Enhanced Location Resolution Algorithm) is used. Here the idea is locators authenticate themselves before sending beacon packet. As other locators know the positions they can detect the compromised locator.

B. HiRLoc

An Improvement to SeRLoc Lazos and poovendran proposed HiRLoc (High Resolution Robust Localization for WSNs) [6]. This algorithm is more accurate because each locator sends beacon information multiple times. Each time locator may change its antenna direction, its communication range or both.

In HiRLoc, sensor s determines the locators of interest LHs as the locators heard by s and it determines an initial estimate for its location. Then, it collects beacon information from locators in rounds. In these rounds, a locator may vary its direction, communication range or both. After that, a region of intersection (ROI) is calculated from the range estimates sent by all locators.

For wormhole, Sybil and compromised network entity attack same technique used in SeRLoc works in HiRLoc also. HiRLoc is more accurate than SeRLoc but creates more overhead and network complexity.

C. Attack Resistant location estimation in sensor networks

Author Donggang et al propose two algorithms to calculate a node's location using distances to other nodes [7]. It is assumed that there is a technique to compute the distance between two nodes and if the distance is affected by attack the proposed two methods will detect the invalid the distance.

1) Attack-Resistant minimum mean square estimation

To detect invalid distances MMSE (minimum mean square estimation) is used. Then, mean square error is

calculated. If the error is above some threshold then the given distance is marked invalid.

2) Voting-based location estimation

In this technique the field is divided into a grid of small cells. Each cell votes its goodness to be the location of the sensor node whose location we want to verify. The centroid of the cells with highest votes is estimated to be the approximate location of sensor node. Any location reference that is far from this estimation is neglected.

D. SecNav

SecNav [8] consists of a set of stations forming a navigation infrastructure which provides radio signals that enable devices to determine their location and to obtain an accurate time reference. Infrastructure stations are synchronized and carefully placed to cover a certain region (each point is within the range of at least four infrastructure stations). It is a broadcasting protocol that does not require the navigation devices (which want to locate themselves) to transmit any messages.

SecNav (Secure Broadcast Localization and Time Synchronization in Wireless Networks) assumes that infrastructure stations are secure against adversary compromises. The main idea of SecNav, as illustrated by Rasmussen et al, is to encode navigation signals using integrity-codes. To ensure the message will contain an equal number of ones and zeros, Manchester encoding is applied. Then, on-o_ keying is applied such that 1 corresponds to a random waveform, while 0 corresponds to silence. Note that an attacker cannot turn a 1 into 0.

E. ROPE

Lazos proposed a scheme called ROPE (Robust Position Estimation in Wireless Sensor Networks) [9]. In this scheme network consists of two kinds of nodes-sensors having Omni-directional antennas and locator having very less density than sensors but very large range radius and equipped with M directional antennas.

In location determination, each unknown node obtains its exact location when it is inside at least one triangle formed by locators, and still estimates its location by center of gravity when it is not inside any triangle. The location verification mechanism verifies the location claims of the unknown nodes. Since every unknown node can communicate with at least one locator, when an unknown node reports data to a locator, the locator can verify the unknown node's position by the execution of the distance bounding protocol.

F. DRBTS

Srinivasan et al proposed Distributed Reputation-based Beacon Trust System (DRBTS) that uses the concept of reputation for excluding anchor nodes [10]. Every anchor node maintains a Neighbor-Reputation-Table (NRT). An anchor node monitors its 1-hop neighborhood for misbehaving anchor nodes, and updates its NRT accordingly. Then, it publishes the NRT enabling other anchor nodes to update their own NRTs, and enabling nearby sensor nodes to determine whether or not to use a given anchor's location information. Sensor nodes can choose some trusted anchor nodes, based on a quorum voting approach. The unknown nodes will only use the anchor node trusted by its neighbor anchor nodes to compute its position.

Algorithm	Encrypton Keys	Use of Anchors	Range free/ Range Based
SeRLoc	Used	Yes	Range Based
HiRLoc	Used	Yes	Range Based
Attack Resistant MMSE	Not Used	No	Range Free
SecNav	Not Used	Yes	Range Free
ROPE	Used	Yes	Range Based
DRBTS	Used	Yes	Range Based

V. CONCLUSIONS

Determining the location of a sensor node in the sensor field is an important task as wireless sensor network does not have a centralized infrastructure to keep track of the positions of sensor nodes. Just getting the location of sensor node can be easy with sensor network also faces many attacks which could result in wrong location values.

The paper discusses the different types of attacks in Wireless Sensor Networks and their effects on the localization scheme. This is helpful to understand how network can get attacked and how to secure it. Also different secure localization schemes are also discussed.

REFERENCES

[1] G. Padmavathi, D. Shanmugapriya, "A survey of attacks security mechanism and Challenges in Wireless Sensor Networks", (IJCSIS) International Journal of Computer Science and Information Security,2009, Vol. 4, No. 1 & 2.

[2] A. Wood and J. Stankovic "A taxonomy for denial-ofservice attacks in wireless sensor networks", in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.

[3] W. Ammar, A. ElDawy, M. Youssef, "Secure Localization in Wireless Sensor Networks: A Survey", July 2009, CoRR abs/1004.3164.

[4] A. Singla, R. Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, April 2013.

[5] L. Lazos and R. Poovendran, "Serloc: secure range-independent localization for wireless sensor networks", WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security, pages 21-30, New York, NY, USA, 2004.

[6] L. Lazos and R. Poovendran, "Hirloc: high-resolution robust localization for wireless sensor networks", IEEE Journal on Selected Areas in Communications, 24(2):233-246, 2006.

[7] D. Liu, P. Ning et. Al., "Attack- Resistant Location Estimation in Wireless Sensor Networks" ACM Trans. Inf. Syst. Secur., 11(4):1-39, 2008.

[8] K. Rasmussen, S. Capkun, and M. Cagalj, "Secnav: secure broadcast localization and time synchronization in wireless networks," MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking, pages 310-313, New York, NY, USA, 2007.

[9] L. Lazos, R. Poovendran, and S.Capkun, "Rope: robust position estimation in wireless sensor networks", IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks, page 43, Piscataway, NJ, USA, 2005.

[10] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation based Beacon Trust System", 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006.